THORGUARD DEFENSE

WHITE PAPER | JUNE 2026

The True Cost of a Cyberattack on Your Firm

What Law Firms, Financial Advisors, and Accounting Practices Need to Know in 2026

A single cyberattack can cost a professional services firm millions of dollars, destroy client trust built over decades, and trigger regulatory consequences that linger for years. Yet most small firms operate without dedicated cybersecurity protection. Not because they are careless, but because they assume the risk does not apply to them.

It does. The data in this paper comes from the most authoritative sources in the field, including the IBM and Ponemon Institute Cost of a Data Breach Report, the Verizon Data Breach Investigations Report, the American Bar Association, the Securities and Exchange Commission, the IRS, and joint advisories from the FBI and CISA. Every figure cited here is traceable to one of those sources, and a full source list appears at the end of this document.

1. The Financial Reality of a Data Breach

Each year IBM and the Ponemon Institute study hundreds of real data breaches and calculate what they actually cost the organizations involved. The 2025 edition, the twentieth year of the study, examined 600 organizations that suffered breaches between March 2024 and February 2025. The findings are stark for American businesses.

$10.22M	$4.56M	16%
Average cost of a data breach in the United States, an all time record (IBM 2025)	Average breach cost for professional services firms, including legal and accounting (IBM 2025)	Share of breaches that began with phishing, the most common entry point (IBM 2025)

The United States has recorded the highest breach costs in the world for fifteen consecutive years. In 2025 the average cost of a US data breach rose 9 percent to $10.22 million, driven largely by higher regulatory fines and rising detection and investigation costs. The global average was $4.44 million.

Professional services firms, a category IBM defines as legal, accounting, and consulting firms, averaged $4.56 million per breach. That is above the global average across all industries.

To be clear, a breach at a firm with 20 employees will not cost ten million dollars. These averages are drawn from organizations of all sizes. But the cost categories scale down with painful consistency. Forensic investigation, legal counsel, client notification, regulatory response, system recovery, and lost business apply to a 15 person firm just as they do to a Fortune 500 company. For a small firm the absolute numbers are smaller, but they hit a business with far less cushion to absorb them.

It is also worth understanding how attackers get in. According to IBM, the most common initial attack vector in 2025 was phishing, a fraudulent email or message designed to trick an employee into handing over credentials or clicking a malicious link. Phishing accounted for 16 percent of breaches and cost an average of $4.8 million per incident. In other words, the most common path into your systems runs through your inbox, not through some exotic technical exploit.

2. Why Professional Services Firms Are a Primary Target

Attackers think like investors. They look for the highest concentration of valuable data behind the weakest defenses. Professional services firms sit exactly at that intersection. A law firm, advisory practice, or accounting firm holds financial records, Social Security numbers, transaction details, and privileged communications for hundreds of clients, often protected by less security than a single mid size retailer.

The Verizon Data Breach Investigations Report, the most widely cited annual study of real breach incidents, makes the pattern clear in its 2026 edition:

- **The human element was present in 62 percent of breaches.** Most successful attacks still depend on a person making a mistake, such as clicking a phishing link, reusing a password, or being manipulated over the phone.
- **Ransomware appeared in 48 percent of breaches,** up from 44 percent the year before. Ransomware is malicious software that locks your files or steals your data and demands payment to restore or withhold it.
- **Small and midsize businesses made up roughly 96 percent of ransomware victims** among cases where the size of the organization was known. Attackers are not focused on Fortune 500 companies. They are focused on firms like yours.
- **The median ransom paid was $139,875,** and 69 percent of victims refused to pay. Refusing is often the right call, but it does not make the incident free. The downtime, recovery work, and client notification still have to be paid for.
- **Exploitation of unpatched software became the single most common way in,** accounting for 31 percent of breaches. Firms that delay routine software updates are leaving a door open.

None of this requires a sophisticated adversary singling out your firm. Most of these attacks are automated and opportunistic. The question attackers are effectively asking is simple. Who has valuable data and has not locked the door?

3. Risks Specific to Law Firms

Law firms concentrate exactly what attackers want. Merger details, litigation strategy, intellectual property, trust account information, and deeply personal client records all live on the same systems. And the profession's own data shows the threat is not hypothetical.

- **29 percent of law firms reported having experienced a security breach,** according to the American Bar Association's 2023 Cybersecurity TechReport, which summarizes the ABA Legal Technology Survey. Breaches in the survey include hacking, malware, lost or stolen devices, and unauthorized access.
- **Another 19 percent of respondents did not know** whether their firm had ever been breached. For a profession built on confidentiality, not knowing is its own kind of exposure.

The ethical stakes are just as serious as the financial ones. ABA Model Rule 1.6(c) requires lawyers to make reasonable efforts to prevent the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. ABA Formal Opinion 483 goes further and addresses a lawyer's obligations when a data breach occurs, including the duty to notify current clients whose material confidential information may have been compromised.

Put plainly, a breach at a law firm is not only an IT incident. It can become an ethics issue, a malpractice exposure, and a client relations crisis at the same time. The duty of confidentiality does not come with an exception for firms that found cybersecurity inconvenient.

4. Risks Specific to Financial Advisors: The New SEC Rules Are Now in Effect

If you are an SEC registered investment adviser, the regulatory ground has shifted under you, and the final deadline has already passed.

On May 16, 2024 the SEC adopted sweeping amendments to Regulation S-P, the rule that governs how firms must protect customer information. Larger firms had to comply by December 3, 2025. Every other covered firm, including registered investment advisers with under $1.5 billion in assets under management, had to comply by June 3, 2026. As of today, these requirements apply to every covered firm regardless of size.

Requirement	What it means for your firm
Written incident response program	You must have documented policies and procedures to detect, respond to, and recover from unauthorized access to customer information. A plan that exists only in someone's head does not count.

Customer notification within 30 days	If sensitive customer information was accessed or used without authorization, or is reasonably likely to have been, you must notify affected customers as soon as practicable and no later than 30 days after becoming aware.
Service provider oversight	You are responsible for overseeing the vendors that handle customer information on your behalf, including ensuring they can notify you of breaches so you can meet your own obligations.
Recordkeeping	You must maintain written records documenting compliance with these requirements. In an examination, if it is not documented, it did not happen.

The SEC is not treating this as paperwork. Its Division of Examinations named Regulation S-P compliance a priority for fiscal year 2026 examinations. And enforcement is already real. In November 2025 the SEC settled charges against M Holdings Securities, an Oregon based broker dealer and investment adviser, after email account takeovers at its branch offices exposed the personal information of roughly 8,500 individuals. The firm was censured and paid a civil penalty of $325,000 for failures under Regulation S-P and the related identity theft rule, Regulation S-ID.

Notably, that case involved conduct from before the new amendments even took effect. The bar has now been raised, and examiners know exactly what to ask for.

5. Risks Specific to Accounting Firms

Accounting and tax practices hold the single most useful data set for identity theft that exists. Names, Social Security numbers, income details, bank accounts, and dependent information sit together in one client file. A criminal who steals a tax firm's client data can file fraudulent returns at scale.

Federal law already treats your firm accordingly:

- **You are a financial institution under federal law.** The IRS and its Security Summit partners remind tax professionals every year that under the Gramm-Leach-Bliley Act, tax and accounting professionals are considered financial institutions and are required to protect customer data.
- **A written security plan is mandatory, not optional.** The FTC Safeguards Rule requires every firm to maintain a written information security plan, designate someone to coordinate it, assess risks, implement and test safeguards, and oversee service providers.
- **Breach reporting obligations apply.** Under FTC rules, a security incident involving the information of 500 or more individuals must be reported to the FTC within 30 days of discovery.

The threat side is just as concrete. The FBI, CISA, and their Australian counterpart maintain a joint #StopRansomware advisory on the BianLian group, a data extortion operation that has hit

organizations across US critical infrastructure sectors and has targeted professional services firms. BianLian is notable because it largely stopped bothering to encrypt files. It simply steals the data and threatens to publish it unless paid. For an accounting firm, the publication threat alone is existential, because the stolen files are your clients' complete financial identities.

6. The Real Impact Goes Beyond the Invoice

Dollar figures understate what a breach actually does to a firm, because the deepest damage is operational and reputational. The IBM 2025 study measured this directly across the breached organizations it examined:

86%	65%	76%
Of breached organizations experienced operational disruption (IBM 2025)	Had still not fully recovered at the time they were studied (IBM 2025)	Of those that did fully recover needed more than 100 days to get there (IBM 2025)

In addition, 32 percent of breached organizations paid a regulatory fine, and the most commonly stolen data type was customer personal information, taken in 53 percent of breaches.

Now translate that into the economics of a professional services firm. Your business runs on billable time and client trust. Operational disruption means partners and staff spending weeks on incident response instead of client work. And the trust dimension is harsher for you than for almost any other industry. Clients hand a law firm, advisor, or CPA their most sensitive information precisely because they believe it will be protected. A breach breaks the exact promise the relationship is built on. Competitors do not need to say a word. The client's next question is simply why they should keep taking the risk.

7. What Effective Protection Actually Looks Like

The encouraging news is that the same research that documents the cost of breaches also documents what reduces it. Effective protection for a small firm is not a single product, and it does not require building an internal IT department. It is a set of layered, managed practices:

- **Train your people and test them.** With the human element involved in 62 percent of breaches, regular security awareness training and simulated phishing exercises target the single largest risk factor. IBM found employee training reduced average breach costs by roughly $192,000.
- **Require multifactor authentication everywhere.** Multifactor authentication means a stolen password alone is not enough to get in, because a second proof such as a phone prompt is required. It is one of the cheapest and most effective controls that exists.
- **Patch promptly.** With unpatched software now the most common entry point in the Verizon data, routine and timely updates close the doors attackers check first.

- **Monitor continuously.** Breaches that are found and contained faster cost dramatically less. IBM found organizations making extensive use of security automation and AI saved an average of $1.9 million per breach and cut 80 days off the breach lifecycle.
- **Have a written, tested incident response plan.** For advisors this is now a legal requirement under Regulation S-P. For tax professionals it is part of the required written security plan. For everyone it is the difference between a controlled response and a panic.
- **Oversee your vendors.** Your IT provider, your software platforms, and your cloud services all touch client data. Regulators increasingly hold you responsible for them.
- **Back up your data and verify the backups work.** Reliable, tested backups are what turn a ransomware incident from a catastrophe into a bad week.

IBM's analysis also found that working with a managed security service provider reduced average breach costs by roughly $128,000. The economics point in one direction. For a firm of 10 to 50 people, professionally managed protection costs a small fraction of what a single incident does.

8. Where to Start

Every firm's exposure is different. The right starting point is not a product purchase. It is an honest assessment of where you stand today. Which systems hold client data. Who can access them and how. Whether your people would recognize a phishing email. Whether you could meet a 30 day notification deadline if something happened tomorrow.

ThorGuard Defense provides exactly that assessment to professional services firms at no cost and with no obligation. We review your current security posture, identify the gaps that matter most for a firm of your size and regulatory profile, and give you a clear, plain English picture of where you stand. If you never speak to us again, you will still walk away knowing more about your firm's risk than most of your competitors know about theirs.

Request your free security assessment at **thorguarddefense.com** or email **norbert@thorguarddefense.com**.

Sources

All statistics and regulatory statements in this paper are drawn from the following sources, listed with enough detail to be independently verified.

IBM Security and Ponemon Institute. Cost of a Data Breach Report 2025. Published July 2025. Available at ibm.com/reports/data-breach. Figures cited: $10.22 million US average breach cost, $4.44 million global average, $4.56 million professional services average, phishing as top initial attack vector at 16 percent with $4.8 million average cost, 86 percent operational disruption, 65 percent not fully recovered, 76 percent of recovered organizations requiring over 100 days, 32 percent paying regulatory fines, customer personal information stolen in 53 percent of breaches, $1.9 million average savings from extensive security AI and automation, approximately $192,000 cost reduction from employee training, and approximately $128,000 cost reduction from use of a managed security service provider.

Verizon. 2026 Data Breach Investigations Report. Published May 2026. Available at verizon.com/business/resources/reports/dbir. Figures cited: human element present in 62 percent of breaches, ransomware involved in 48 percent of breaches, small and midsize businesses representing approximately 96 percent of ransomware victims where organization size was known, 69 percent of victims declining to pay, median ransom payment of $139,875, and vulnerability exploitation as the top initial access vector at 31 percent.

American Bar Association, Legal Technology Resource Center. 2023 Cybersecurity TechReport, summarizing the ABA Legal Technology Survey Report. Available at americanbar.org. Figures cited: 29 percent of respondents reporting a security breach and 19 percent not knowing whether their firm had experienced one.

American Bar Association. Model Rule of Professional Conduct 1.6(c) and ABA Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack, issued October 17, 2018.

U.S. Securities and Exchange Commission. Amendments to Regulation S-P, adopted May 16, 2024, Release No. 34-100155. Compliance dates of December 3, 2025 for larger entities and June 3, 2026 for all other covered institutions.

U.S. Securities and Exchange Commission, Division of Examinations. Fiscal Year 2026 Examination Priorities, published November 2025.

U.S. Securities and Exchange Commission. Administrative proceeding against M Holdings Securities, Inc., Release No. 34-104255, settled November 25, 2025. Censure and $325,000 civil penalty for violations of Regulation S-P Rule 30(a) and Regulation S-ID Rule 201. Available at sec.gov.

Internal Revenue Service and Security Summit. News release IR-2025-79, July 29, 2025, on the Written Information Security Plan requirement for tax professionals under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule, including the requirement to report incidents affecting 500 or more individuals to the FTC within 30 days. Available at irs.gov.

FBI, CISA, and the Australian Cyber Security Centre. Joint Cybersecurity Advisory AA23-136A, #StopRansomware: BianLian Ransomware Group, updated November 20, 2024. Available at cisa.gov.

ThorGuard Defense LLC | norbert@thorguarddefense.com | thorguarddefense.com | Chicago, IL